Cybersecurity in the Era of Neo-Banking

The banking industry has undergone continuous transformation since the dual shock of the 2008 Global Financial Crisis and the emergence of the digital platform economy. These shifts have introduced new strategic priorities that demand careful consideration, especially in the context of digital innovation and cybersecurity.

The Traditional Banking Challenges

The failure to consider the unique ability of banks to create new money through lending is part of a much broader misunderstanding of how banks operate and the role they play in money creation. This misunderstanding stems from erroneous assumptions contained in the financial intermediation theory of banking that has been dominant across most developed economies since the 1960s, which maintains that banks are simply intermediaries that collect deposits that are then lent out and are thus not materially different from other nonbanking firms.

A Brief History

Over the past century and a half, our understanding of how banks operate has shifted significantly, shaped by three main theories that each dominated at different times. The earliest of these, the **credit creation theory**, gained traction in the late 19th and early 20th centuries. It argued that banks have the power to generate money "from nothing" simply by issuing loans, a process known (as *creatio ex nihilo)*. This perspective held sway until the 1930s.

By the mid-20th century, the focus had shifted to the **fractional reserve theory**. Prevailing from the 1930s through the 1960s, this model proposed that while individual

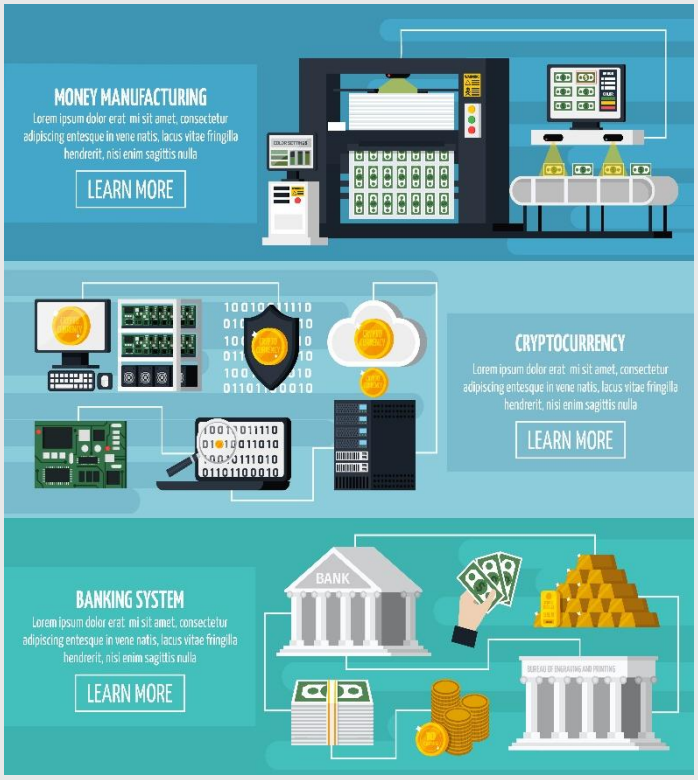
banks couldn't create money on their own, the banking system as a whole could expand the money supply through a multiplier effect. Banks, in this view were essentially intermediaries that accepted deposits and loaned them out, with their collective activity enabling broader monetary expansion.

Then came the **financial intermediation theory**, which rose to prominence in the 1960s. This approach downplayed the distinctiveness of banks, portraying them as similar to any other financial institution. According to this theory, banks simply moved funds from savers to borrowers without playing any direct role in money creation, either individually or collectively.

The 2008 Financial Crisis had triggered the introduction of unconventional monetary policies, such as quantitative easing which significantly compressed banks profit margins.
Regulatory bodies introduced a wave of reforms such as Basel III, the Dodd-Frank Act, and the second Markets in Financial Instruments Directive (MiFID II), all of which increased the compliance burden for banks. Simultaneously, policymakers, particularly in Europe, sought to stimulate innovation in financial services by supporting new market entrants such as financial technology firms (fintech's) and major technology companies (big techs).

Regulatory frameworks like the European Commission's Payment Services Directive 2 (PSD2), the UK's Open Banking Standard, and the General Data Protection Regulation (GDPR) were all implemented in 2018 reshaping data access, consumer rights, and cybersecurity requirements across the sector.

Key Technology Challenges


MONEY MANUFACTURING
Lorem ipsum dolor erat mi sit amet, consectetur adipiscing entesque in vene natis, lacus vitae fringilla hendrerit, nisi enim sagittis nulla
LEARN MORE
CRYPTOCURRENCY
Lorem ipsum dolor erat mi sit amet, consectetur adipiscing entesque in vene natis, lacus vitae fringilla hendrerit, nisi enim sagittis nulla
LEARN MORE
BANKING SYSTEM
Lorem ipsum dolor erat mi sit amet, consectetur adipiscing entesque in vene natis, lacus vitae fringilla hendrerit, nisi enim sagittis nulla
LEARN MORE
BANK

Technological advancements in AI, Cloud, and Blockchain have further accelerated change.
And a new era of digitally native generation, more inclined towards access-based consumption than ownership has embraced the sharing economy and driven demand for seamless, technology-driven services.
In response, many firms across sectors have adopted a platform-based approach, steering in the platform economy era. This new environment saw the rise of fintech's, backed by venture capital and innovation ecosystems, and big techs, leveraging their existing infrastructure and trust to offer financial services such as Apple Pay, Google Pay, and Amazon Pay. These challengers benefited not only from technological capabilities but also from a consumer base increasingly sceptical of traditional banks following the 2008 crisis.

Since then the growth in the financial sector had remained relatively subdued. During the period of regulatory reform and increased scrutiny, U.S. regulators effectively imposed an informal moratorium on the issuance of new bank charters. This position began to shift in 2017, when a small number of new charter applications received approval. The easing of restrictions has the potential to reinvigorate the sector, offering opportunities for financial services to evolve in ways similar to financial technology firms (fintech's), which leveraged innovation as a key competitive advantage during the intervening years. However, it is worth noting that banks outside the U.S. have generally been more proactive and successful in adopting and integrating fintech innovations so far.

Neo Banking Cybersecurity Challenges

In the awake of all this, cybersecurity has become an essential concern. As banks and new entrants digitise services and manage increasingly complex data ecosystems, the security of digital infrastructure and customer data is critical. The convergence of financial services and technology has expanded the attack surface for cyber threats, requiring institutions to adopt more robust security frameworks, invest in cyber resilience, and navigate an evolving regulatory environment focused on data protection and operational integrity.

The expanding scale and complexity of the financial ecosystem marked by growing interconnectivity among diverse stakeholders has introduced new vulnerabilities, including account takeovers, insider threats, and ransomware attacks to name some.

As financial institutions modernise their infrastructure to better serve consumers and businesses, these developments will demand significant innovation in cybersecurity. While some advancements are already being piloted, none have yet emerged as a definitive new standard. Much like environmental impact assessments are integral to planning in the manufacturing sector, cybersecurity assurance must become a core consideration in the adoption of new technologies.

The escalating severity of cyberattacks over the past decade, coupled with the increasing reliance on automation across industries, has drawn attention from leading governance bodies such as the National Association of Corporate Directors (NACD) and the National Institute of Standards and Technology (NIST). The NACD argues that while boards often address cybersecurity in isolated agenda items, true resilience requires embedding cybersecurity within broader strategic discussions. NIST similarly stresses that cybersecurity management should not remain purely operational, it must be fully integrated into enterprise risk frameworks.

Across all governance guidance, the message is consistent, proper and robust cybersecurity controls are fundamental to managing enterprise risk.
As this principle extends to technology specially within the AI readiness, governance more broadly, financial institutions and businesses across sectors are becoming increasingly reliant on data integrity and computational safeguards to underpin their risk management efforts.

Investments in modern transaction systems and cybersecurity are vital for mitigating risk. However, the broader adoption of automation introduces a paradox. While it reduces certain operational risks, it may amplify others, transforming frequent, low-impact incidents into rare but catastrophic failures. The Bank for International Settlements has highlighted that not all automation related risks are internal; disruptions to external service providers, such as telecommunications networks, can have profound consequences.
For example, vulnerabilities in undersea cable infrastructure illustrate how financial services are dependent on other sectors to ensure transaction continuity and safety.

This interconnectedness has reshaped our core banking in how identity is authenticated, and transactions are routed. Customers may now be recognised through a range of identifiers, such as internal directories, email addresses, bank account numbers, merchant credentials, NFC, credit card numbers, fintech accounts, or third-party P2P payment services. As these channels gain trust and prominence, digital identity itself may evolve into a competitive differentiator. For instance, email providers could increasingly partner with banks to offer cybersecurity features that prevent account takeovers, especially those executed via compromised password reset functions.

Closing Words

Think of cybersecurity as a perpetual change to a “hamster wheel”, a relentless cycle with no clear end in sight. James P. Carse, a professor at New York University, proposed a compelling framework for understanding how systems operate, a concept later popularised by Simon Sinek. Carse distinguished between two types of games, a finite and infinite.

Finite games are defined by established rules, identifiable players, and a clear endpoint typically resulting in a winner and a loser. Chess, for instance, exemplifies a finite game. Its rules are universally recognised, the participants are clearly defined, and victory is unambiguous. Infinite games, by contrast, operate with no fixed rules, an ever changing set of players some known, others not and no definitive endpoint. The objective in an infinite game is not to win, but to persist and adapt. Consider the financial system, where regulatory frameworks vary widely across jurisdictions, new actors continually emerge, and the landscape evolves in unpredictable ways.

Chadi Saliby

References:

- Banking in the Age of the Platform Economy, May 2023.
- https://www.bis.org/bcbs/basel3.htm
- https://www.bbva.com/en/francisco-gonzalez-the-future-of-banking-is-decided-in-places-like-this-one/
- https://www.bloomberg.com/news/articles/2021-05-27/fintech-unicorn-stash-is-said-to-weigh-options-for-going-public%23xj4y7vzkg
- *New Players in Entrepreneurial Finance and Why They are There, Small Business Economics.* 2018.
- Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions, December 2018.